Linear codes using skew polynomials with automorphisms and derivations

Delphine Boucher, Félix Ulmer

Linear codes using skew polynomials with automorphisms and derivations

D. Boucher and F. Ulmer *

May 30, 2011

Abstract

In this work the definition of codes as modules over skew polynomial rings of automorphism type is generalized to skew polynomial rings whose multiplication is defined using an automorphism and an inner derivation. This produces a more general class of codes which, in some cases, produce better distance bounds than skew module codes constructed only with an automorphism. Extending the approach of Gabidulin codes, we introduce new notions of evaluation of skew polynomials with derivations and the corresponding evaluation codes. We propose several approaches to generalize Reed Solomon and BCH codes to module skew codes and for two classes we show that the dual of such a Reed Solomon type skew code is an evaluation skew code. We generalize a decoding algorithm due to Gabidulin for the rank matrix and derive families of MDS and MRD codes.

Keywords: error-correcting codes, decoding, finite fields, skew polynomial rings

1 Skew module codes with derivation

Let A be a ring with an automorphism θ, then a θ-derivation is a map $\delta_\theta : A \to A$ such that for all a and b in A:

$$\begin{aligned} \delta_\theta(a+b) &= \delta_\theta(a) + \delta_\theta(b) \\ \delta_\theta(ab) &= \delta_\theta(a)b + \theta(a)\delta_\theta(b). \end{aligned}$$

According to [14] the most general skew polynomial rings in the variable X over ring A, whose elements are written $\sum_{i=0}^{n} a_i X^i$, are defined with the usual addition of polynomials and a multiplication that follows the commuting rule $Xa = \theta(a)X + \delta(a)$. We note the resulting ring $A[X;\theta,\delta]$ and, if A is a division ring, the ring $A[X;\theta,\delta]$ is a left and right euclidean ring in which left and right gcd and lcm exist [14].
If A is a finite field $\mathbb{F}_q$, then all θ-derivations are of the form $\delta_\beta(a) = \beta(\theta(a) - a)$ where $\beta \in \mathbb{F}_q$ and are therefore uniquely determined by $\beta \in \mathbb{F}_q$ (cf. [16], Corollary of Proposition 8). We denote $(\mathbb{F}_q)^\theta$ the fixed field of θ in $\mathbb{F}_q$.

*IRMAR (UMR 6625), Université de Rennes 1, Campus de Beaulieu, F-35042 Rennes Cedex

In the following we will consider modules over $R = \mathbb{F}_q[X;\theta,\delta_\beta]$ and in particular submodules $Rg/Rf \subset R/Rf$. We have $Rf \subset Rg$ if and only if g is a right factor of f and in this case Rg/Rf is a submodule of R/Rf which is cyclic and generated as a left R-module by $g + Rf$. Therefore the left R-submodule $Rg/Rf \subset R/Rf$ is a $\mathbb{F}_q$-vector subspace of dimension $\deg(f) - \deg(g)$ of the $\mathbb{F}_q$-vector space R/Rf of dimension $\deg(f)$. In analogy to classical cyclic codes, we associate to an element $\sum_{i=0}^{n-1} a_i X^i$ in the quotient module R/Rf the 'word' $(a_0, a_1, \ldots, a_{n-1}) \in {\mathbb{F}_q}^n$.

Definition 1 *Let $R = \mathbb{F}_q[X;\theta,\delta_\beta]$ and $f \in R$ be of degree n. A* **module (θ,δ)-code** *$\mathcal{C}$ is a left R-submodule $Rg/Rf \subset R/Rf$ in the basis $1, X, \ldots, X^{n-1}$ where g is a right divisor of f in R. The length of the code is $n = \deg(f)$ and its dimension is $k = \deg(f) - \deg(g)$, we say that the code $\mathcal{C}$ is of type $[n,k]_q$. If the minimal distance of the code is d, then we say that the code $\mathcal{C}$ is of type $[n,k,d]_q$. We denote this code $\mathcal{C} = (g)_{n,\theta,\delta_\beta}$.*

The above module codes generalize the codes defined in [4] and are also considered in [5]. As we shall see, there is a strong connection to Gabidulin codes (cf. [8]). A generator matrix of the code is given by the coefficients of $g, X\cdot g, \ldots, X^{k-1}\cdot g$ and can be computed using the rule $Xa = \theta(a)X + \beta(\theta(a) - a)$ for $a \in \mathbb{F}_q$. Note that this generator matrix depends only on the degree n of f, which justifies the notation $\mathcal{C} = (g)_{n,\theta,\delta_\beta}$.

In this paper we will consider both the Hamming distance and the *rank distance* introduced in [8] which is well adapted to our situation. Consider an $\mathbb{F}_q$-vector space $V = (\mathbb{F}_q)^m$ over $\mathbb{F}_q$ (like the codes we consider) and a subfield $(\mathbb{F}_q)^\theta \subset \mathbb{F}_q$. The rank of $\gamma = (\gamma_1, \ldots, \gamma_m) \in V$, denoted $\mathrm{rank}(\gamma)$, is the dimension of the $(\mathbb{F}_q)^\theta$-vector space spanned by $\gamma_1, \ldots, \gamma_m$. The relation $d_{rank}(\gamma,\tilde{\gamma}) = \mathrm{rank}(\gamma - \tilde{\gamma})$ defines a distance over $V = (\mathbb{F}_q)^m$. If d_H denotes the classical Hamming distance, then $d_{rank}(\gamma,\tilde{\gamma}) \leq d_H(\gamma,\tilde{\gamma})$ (cf. [1]).

It is well known that there exists a change of variable which transforms a skew polynomial ring $A[X;\theta,\delta]$ over division rings A into either $A[Z;\theta]$ or $A[Z;\delta]$ (cf. [7], page 295). If $A = \mathbb{F}_q$ and $\delta_\beta \neq 0$, then after the change of variable $Z = X + \beta$ we obtain a pure automorphism ring $\mathbb{F}_q[Z;\theta]$. This corresponds to the bijective ring homomorphism

$$\begin{aligned} \mathcal{H} : \mathbb{F}_q[X;\theta,\delta_\beta] &\rightarrow \mathbb{F}_q[Z;\theta] &(1)\\ \sum a_i\, X^i &\mapsto \sum a_i\, (Z-\beta)^i\,. &(2)\end{aligned}$$

The morphism $\mathcal{H}$ induces a map (which we also denote $\mathcal{H}$) from an $[n,k]$ module code $\mathcal{C} = (g)$ over $\mathbb{F}_q[X;\theta,\delta_\beta]$ with $\beta \neq 0$ to a $[n,k]$ module code $\tilde{\mathcal{C}} = (\mathcal{H}(g))$ over $\mathbb{F}_q[Z;\theta]$ via

$$\sum_{i=0}^{n-1} c_i\, X^i \;\mapsto\; \sum_{i=0}^{n-1} c_i\, (Z-\beta)^i = \sum_{i=0}^{n-1} \tilde{c}_i\, Z^i.$$

Computing recursively the coefficients of $(X+\beta)^i = \sum_{j=0}^{i} a_{i+1,j+1} X^j$ using

$$(X+\beta)^{i+1} = (X+\beta)\sum_{j=0}^{i} a_{i+1,j+1}X^j = \sum_{j=0}^{i} \theta(a_{i+1,j+1})(X+\beta)X^j$$

we obtain the following link between the generating matrices of the codes

$$G_{g,n,\theta,\delta_\beta} = G_{\mathcal{H}(g),n,\theta} \times A_{n,n}(\beta),$$

where $A_{n,n}(\beta)$ is a lower unit triangular $n \times n$ matrix over $(\mathbb{F}_q)^\theta(\beta)$ whose entries $a_{i,j}$ $(j < i)$ are given by $a_{i+1,j+1} = \theta(a_{i,j}) + \beta\theta(a_{i,j+1})\,(1 < j < i)$, $a_{i+1,1} = \beta\theta(a_{i,1})\,(1 < j)$.

The corresponding $\mathbb{F}_q$-linear map between the codes $(g)_{n,\theta,\delta_\beta}$ and $(\mathcal{H}(g))_{n,\theta}$ does not preserve the Hamming distance (for $\beta \neq 0$ the weight of $\mathcal{H}(X)$ is 2) nor the rank distance. We shall see that the consideration of $\mathbb{F}_q[X;\theta,\delta_\beta]$ with $\beta \neq 0$ indeed produces new codes which are not module codes over $\mathbb{F}_q[X;\theta]$. From the above matrix $A_{n,n}(\beta)$ we see that the rank is preserved when $\beta \in (\mathbb{F}_q)^\theta$.

The map $\mathcal{H}$ will be also useful in the context of evaluation codes introduced in the section 3.

Proposition 1 *For any $\sigma \in \mathrm{Aut}(\mathbb{F}_q)$ the following map is a ring isomorphism*

$$\begin{array}{rcl} \varphi_\sigma : \mathbb{F}_q[X;\theta,\delta_\beta] & \to & \mathbb{F}_q[X;\theta,\delta_{\sigma(\beta)}] \\ \displaystyle\sum_{i=0}^{n} a_i X^i & \mapsto & \displaystyle\sum_{i=0}^{n} \sigma(a_i) X^i \end{array}$$

Proof: The map φ_σ is an isomorphism of the corresponding additive groups, so we need to check the multiplicative rule. We have $\varphi_\sigma(aX) = \sigma(a)X = \varphi_\sigma(a)\varphi_\sigma(X)$. In order to verify the reverse multiplication rule, we note that, since the group $\mathrm{Aut}(\mathbb{F}_q)$ is abelian, we always have $\sigma\theta = \theta\sigma$:

$$\begin{array}{rcl} \varphi_\sigma(X)\varphi_\sigma(a) & = & X\sigma(a) \,=\, (\theta\circ\sigma)(a)X + \sigma(\beta)\left((\theta\circ\sigma)(a) - \sigma(a)\right) \\ & = & \sigma(\theta(a))X + \sigma\left(\beta(\theta(a) - a)\right) \,=\, \varphi_\sigma(Xa) \end{array}$$

□

This shows that the following map

$$\begin{array}{rcl} \varphi_\sigma : (g)_{n,\theta,\delta_\beta} & \to & (\varphi_\sigma(g)))_{n,\theta,\delta_{\sigma(\beta)}} \\ (a_0, a_1, \ldots, a_{n-1}) & \mapsto & (\sigma(a_0), \sigma(a_1), \ldots, \sigma(a_{n-1})) \end{array}$$

has the property that for a and b in $(g)_{n,\theta,\delta_\beta}$, $\varphi_\sigma(a+b) = \varphi_\sigma(a) + \varphi_\sigma(b)$ and for $\lambda \in \mathbb{F}_q$, $\varphi_\sigma(\lambda \cdot a) = \sigma(\lambda)\varphi_\sigma(a)$. Since the map φ_σ preserves the Hamming distance of linear codes, it is a semilinear isometry for the Hamming distance.

This new class of codes is more general than the codes obtained using skew polynomials of automorphism type for which $\beta = 0$. In the following tables we give the parameters of codes which reach the best known Hamming distances over $\mathbb{F}_4$, $\mathbb{F}_8$ and $\mathbb{F}_9$ thanks to a nonzero derivation and do not reach them with a zero derivation (tables for codes over $\mathbb{F}_4$ also appear in [5]). Because of the above semilinear isometry φ_σ, we only included codes for one element of each orbit of $\beta \in \mathbb{F}_q^*$ under the action of θ.

n	k	d	$\beta = 0$	$\beta = 1$	$\beta = a$
5	3	3	2	2	3
15	8	6	5	5	6
15	12	3	2	2	3
16	10	5	4	5	4
21	13	6	5	5	6
31	27	3	2	2	3
⋮	⋮	⋮	⋮	⋮	⋮
40	36	3	2	2	3

Table 1: $\mathbb{F}_4$

n	k	d	$\beta = 0$	$\beta = 1$	$\beta = a$	$\beta = a^3$
22	19	3	2	3	3	3
23	20	3	2	3	3	2
⋮	⋮	⋮	⋮	⋮	⋮	⋮
30	27	3	2	3	3	2

Table 2: $\mathbb{F}_8$

n	k	d	$\beta = 0$	$\beta = 1$	$\beta = a$	$\beta = a^2$	$\beta = a^4$	$\beta = a^5$
9	3	7	6	7	6	7	7	6
10	4	7	6	6	6	7	6	6
9	5	5	4	4	4	5	4	4
10	6	5	4	4	4	5	4	4
27	24	3	2	3	3	2	3	3
⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮
30	27	3	2	3	3	2	3	3

Table 3: $\mathbb{F}_9$

2 Wronskian and Vandermonde matrices

Like in the commutative case, many constructions of codes are based on the notion of the evaluation of a polynomial. We follow the definition of an evaluation given in [11] (where noncommutative fields of coefficients are also considered):

Definition 2 *Let K be a division ring, $\theta \in \mathrm{Aut}(K)$ and δ a θ-derivation. For $f = \sum a_i X^i \in K[X;\theta,\delta]$ and $\alpha \in K$ the* **(right) remainder evaluation** *of f at α is denoted $f(\alpha)$ and is defined as the remainder of the right division of f by $X-\alpha$. We also define $N_i^{\theta,\delta}(\alpha)$ recursively as*

$$\begin{array}{rcl} N_0^{\theta,\delta}(\alpha) & = & 1 \\ N_{i+1}^{\theta,\delta}(\alpha) & = & \theta(N_i^{\theta,\delta}(\alpha))\,\alpha + \delta(N_i^{\theta,\delta}(\alpha)) \end{array}$$

Lemma 1 *([11], Proposition 2.9) Let K be a division ring, $\theta \in \mathrm{Aut}(K)$ and δ a θ-derivation. For $f = \sum a_i X^i \in K[X;\theta,\delta]$ and $\alpha \in K$ we get $f(\alpha) = \sum a_i N_i^{\theta,\delta}(\alpha)$.*

In the following θ will play the same role for the ring $K[X;\theta]$ as $\delta \neq 0$ for the ring $K[X;\theta,\delta]$. We therefore introduce the notation:

$$\mathcal{D} = \left\{ \begin{array}{lll} \theta & if & \delta = 0 \\ \delta & if & \delta \neq 0 \end{array} \right.$$

and associate to $f = \sum a_i X^i$ the operator $\mathcal{L}_f = \sum a_i \mathcal{D}^i$ in the ring $K[\mathcal{D};\circ] = \{\sum_{i=0}^n a_i \mathcal{D}^i \mid a_i \in K\}$, where the addition is the usual addition and the multiplication is the composition of operators.

Lemma 2 *Let K be a division ring, $\theta \in \mathrm{Aut}(K)$ and δ a θ-derivation. The map*

$$\begin{array}{rcl} \psi\colon K[X;\theta,\delta] & \to & K[\mathcal{D};\circ] \\ f = \displaystyle\sum_{i=0}^{n} a_i X^i & \mapsto & \mathcal{L}_f = \displaystyle\sum_{i=0}^{n} a_i \mathcal{D}^i \end{array}$$

is a morphism of rings.

From ([10], Lemma 1(2) and [11] Proposition 2.9(4)) we obtain for $0 \neq a \in K$ that $N_i^{\theta}(\mathcal{D}(a)a^{-1}) = \mathcal{D}^i(a)a^{-1}$. Therefore, for $0 \neq a \in K$, we have $f(\mathcal{D}(a)a^{-1}) = \sum a_i N_i^{\theta,\delta}(\mathcal{D}(a)a^{-1}) = 0$ if and only if $\sum a_i \mathcal{D}^i(a) = 0$. This shows that f corresponds to a generalized Ricatti equation of $\mathcal{L}_f$.

Definition 3 *Consider $f = \sum a_i X^i \in K[X;\theta,\delta]$ and $y \in K$, the* **operator evaluation** *of f at $y \in K$ is $\mathcal{L}_f(y)$. If $\mathcal{L}_f(y) = 0$, then y is a solution of $\mathcal{L}_f(Y) = 0$.*

For a field extension $K \subset F$ together with an extension of θ and δ to K we can consider the operator evaluation of $f \in K[X;\theta,\delta]$ at $y \in F$. We will be interested in the case $\mathbb{F}_q[X;\theta,\delta_\beta]$. For an extension $\mathbb{F}_q \subset \mathbb{F}_{q^s}$ we extend an automorphism $a \mapsto a^m$ of $\mathbb{F}_q$ to the corresponding automorphism $a \mapsto a^m$ of $\mathbb{F}_{q^s}$, extending δ_β accordingly.

Definition 4 *([11], page 321) Let K be a division ring, $\theta \in \mathrm{Aut}(K)$ and δ a θ-derivation. Let $A = \{\alpha_1, \ldots, \alpha_n\} \in K^n$. The (θ, δ)-Vandermonde matrix of A is defined by*

$$V_n^{\theta,\delta}(A) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ N_1^{\theta,\delta}(\alpha_1) & N_1^{\theta,\delta}(\alpha_2) & \cdots & N_1^{\theta,\delta}(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ N_{n-1}^{\theta,\delta}(\alpha_1) & N_{n-1}^{\theta,\delta}(\alpha_2) & \cdots & N_{n-1}^{\theta,\delta}(\alpha_n) \end{pmatrix}$$

A closely related matrix is the following generalization of the Wronskian matrix

$$\mathrm{Wr}_n^{\theta,\delta}(y_1, \ldots, y_n) = \begin{pmatrix} y_1 & y_2 & \cdots & y_{n+1} \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \mathcal{D}(y_n) \\ \vdots & & & \\ \mathcal{D}^{n-1}(y_1) & \mathcal{D}^{n-1}(y_2) & \cdots & \mathcal{D}^{n-1}(y_n) \end{pmatrix}.$$

We now summarize some results, most of them from [11], which allow to control the rank of the (θ, δ)-Vandermonde matrix.

Definition 5 *([11]) For a field K and a skew polynomial ring $K[X; \theta, \delta]$ the $(\theta, \delta)-$ conjugacy class of an element $a \in K$ is the set of all its conjugates $a^c := \frac{\theta(c)}{c} a + \frac{\delta(c)}{c}$ where c is taken over all $K - \{0\}$.*

Note 1 *For a finite field $\mathbb{F}_q = \mathbb{F}_{p^N}$ with p prime, $\theta(a) = a^{p^m}$ and $r = gcd(m, N)$ the formula is $a^c := \frac{\theta(c)}{c}(a + \beta) - \beta$. If $a = -\beta$ the $(\theta, \delta)-$ conjugacy class of a is reduced to $\{a\}$ and if $a \neq -\beta$, it has as many elements as the set $\{\frac{\theta(c)}{c}, c \in \mathbb{F}_q^*\}$ namely, $\frac{p^N-1}{p^r-1}$ elements. So we get p^r conjugacy classes : the conjugacy class of $-\beta$ which is a single class and $p^r - 1$ classes with $\frac{p^N-1}{p^r-1}$ elements for each class. In particular, if θ is the Frobenius automorphism ($m = r = 1$), then there are p conjugacy classes.*

Note 2 *As pointed out in [11], the $(\theta, \delta)-$ conjugacy class of 0 is the set of elements of K that are logarithmic derivatives of elements of K. If $\delta = 0$, then $\alpha \in \mathbb{F}_q$ belongs to the conjugacy class of 1 if and only if $\exists a \in \mathbb{F}_q$ such that $\alpha = \frac{\theta(a)}{a}$. If $q = 2^N$ and $\theta : a \mapsto a^2$, then $\frac{\theta(a)}{a} = a$, showing that there are exactly two conjugacy classes: the class of 1 which is $\mathbb{F}_{2^N} \setminus \{0\}$ and the class of 0 which is $\{0\}$.*

Definition 6 *([11], page 3.14) Let K be a division ring with an automorphism θ, a θ-derivation δ and $a \in K$. Then $\mathcal{C}^{\theta,\delta}(a) = \{c \in K^* \mid a^c = a\} \cup \{0\}$.*

From [11], Lemma 3.2 we get that $\mathcal{C}^{\theta,\delta}(a)$ is a division subring of K. If K is a commutative field we recover classical notions:

1. If $\delta = 0$, then $\mathcal{C}^{\theta,\delta}(1) = \{c \in K \mid \theta(c) = c\}$ is the fixed field K^θ of K under θ.
2. If $\delta \neq 0$, then $\mathcal{C}^{\theta,\delta}(0) = \{c \in K \mid \delta(c) = 0\}$ is the subfield of constants $\ker_K(\delta)$ of K for δ.

Theorem 1 *([11], Theorem 4.5 page 323 and [11], page 321)) Let K be a division ring with an automorphism, θ, δ a θ-derivation and $a \in K$. Then, for any $\{y_1, \ldots, y_n\} \subset K^*$, we have* $\operatorname{rank}(V_n^{\theta,\delta}(a^{y_1}, \ldots, a^{y_n})) = \dim_{\mathcal{C}^{\theta,\delta}(a)}(y_1, \ldots, y_n)$. *Let $A = A_1 \cup \cdots \cup A_r$ be the partition of $A \subset K$ into (θ, δ)-conjugacy classes. Then* $\operatorname{rank}(V^{\theta,\delta}(A)) = \sum_{i=1}^{r} \operatorname{rank}(V^{\theta,\delta}(A_i))$.

Corollary 1 *Let K be a field and $f = \sum_{i=0}^{n} a_i X^i \in K[X; \theta, \delta]$ nonzero of degree n. Then*

1. *If $\delta = 0$, the solution space of $\mathcal{L}_f(Y) = 0$ is a vector space of dimension at most n over the fixed field K^θ of K under θ.*
2. *If $\delta \neq 0$, the solution space of $\mathcal{L}_f(Y) = 0$ is a vector space of dimension at most n over the subfield of constants* $\ker_K(\delta)$ *of K for δ.*

Proof: We already noted that the solution space is a vectorspace over K^θ, resp. $\ker_K(\delta)$. Suppose that $L_f(Y) = \left(\sum_{i=0}^{n} a_i \mathcal{D}^i\right)(Y) = 0$ has $n+1$ solutions $y_1, \ldots, y_{n+1}$, then $(a_0, \ldots, a_n)$ is a nonzero vector in the kernel of $\operatorname{Wr}_{n+1}(y_1, \ldots, y_{n+1})$.

1. If $\delta = 0$, then ((4.12) page 325 of [11]) the following matrix is of determinant 0

$$\operatorname{Wr}_{n+1}^{\theta}(y_1, \ldots, y_{n+1}) \cdot \begin{pmatrix} \frac{1}{y_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \frac{1}{y_{n+1}} \end{pmatrix} = V_{n+1}^{\theta,\delta}(1^{y_1}, \ldots, 1^{y_{n+1}}).$$

   From the above theorem we get that $y_1, \ldots, y_{n+1}$ are linearly dependent over K^θ.

2. If $\delta \neq 0$, then ((4.8) page 325 of [11]) the following matrix is of determinant 0

$$\operatorname{Wr}_{n+1}^{\theta,\delta}(y_1, \ldots, y_{n+1}) \cdot \begin{pmatrix} \frac{1}{y_1} & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \frac{1}{y_{n+1}} \end{pmatrix} = V_{n+1}^{\theta,\delta}(0^{y_1}, \ldots, 0^{y_{n+1}})$$

   From the above theorem we get that $y_1, \ldots, y_{n+1}$ are linearly dependent over $\ker_K(\delta)$.

□

The operator $\mathcal{L}(Y)$ whose solution space is spanned by $y_1, y_2, \ldots, y_n$ can be obtained by expanding $|\operatorname{Wr}_{n+1}^{\theta,\delta}(y_1, \ldots, y_n, Y)|$ along the last column. In a similar way, in order to construct the polynomial $f \in K[X; \theta, \delta]$ of minimal degree such that $f(\alpha_1) = \ldots = f(\alpha_n) = 0$ we simply consider $\operatorname{lclm}_{1 \leq i \leq n}(X - \alpha_i) \in K[X; \theta, \delta]$. It corresponds to the minimal polynomial defined in Theorem 8 of [10] or page 326 of [11].

Theorem 2 ([10], [11]) *Let K be a division ring with an automorphism, $a \in K$ and θ, δ a θ-derivation. Let $A = \{\alpha_1, \ldots, \alpha_n\} \in K^n$. Let $g_A = \operatorname{lclm}_{1 \leq i \leq n}(X - \alpha_i) \in K[X; \theta, \delta]$, then* $\deg(g_A) = \operatorname{rank}\left(\mathrm{V}_{\mathrm{n}}^{\theta,\delta}(\mathrm{A})\right)$.

Suppose that $q = q_0^t$ and consider $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ given by $a \mapsto a^{q_0}$. The fixed field $(\mathbb{F}_q)^\theta$ of θ is $\mathbb{F}_{q_0}$. We associate to $\mathcal{L}_f(Y) = \sum_{i=0}^n a_i \mathcal{D}^i$ the commutative *affine linearized polynomial* $\ell(Z) \in \mathbb{F}_q[Z]$ by expressing the action of the automorphism θ and the derivation $\delta_\beta = \beta(\theta - id)$:

1. If $\delta = 0$, then $\mathcal{L}_f(Y) = \sum_{i=0}^n a_i \theta^i$ (cf. Section 5 of [12] or "p-polynomials" in [15])

$$\ell(Z) \;=\; a_n\, Z^{(q_0)^n} \,+\, \ldots \,+\, a_1 Z^{q_0} \,+\, a_0\, Z \;\in \mathbb{F}_q[Z].$$

2. If $\delta \neq 0$ then $\mathcal{L}_f(Y) = \sum_{i=0}^n a_i(\beta(\theta - id))^i \;=\; \sum_{i=0}^n \ell_i(a_0, \ldots, a_n, \beta)\theta^i$ where the coefficients $\ell_i(a_0, \ldots, a_n, \beta)$ can be explicitly computed and in particular $\ell_0(a_0, \ldots, a_n, \beta) = \sum_{i=0}^n (-1)^i \beta^i a_i$. Therefore $\ell(Z) \;=\; \sum_{i=0}^n \ell_i(a_0, \ldots, a_n, \beta) Z^{(q_0)^i} \;\in \mathbb{F}_q[Z]$.

Definition 7 *The multiplicity of a solution, a, of $\mathcal{L}_f(Y)$ is the order of a, as a root of the associated linearized polynomial $\ell(Z)$.*

The proof of [[6] Theorem 1] generalizes to

Theorem 3 *Consider $f = \sum_{i=0}^n a_i X^i \in \mathbb{F}_q[X; \theta, \delta_\beta]$ and the corresponding $\mathcal{L}_f$. There exists a finite field extension $\mathbb{F}_{q^s}/\mathbb{F}_q$ which contains all the roots of $\ell_L(Y) = 0$ and the $(\mathbb{F}_q)^\theta$-subspace of $\mathbb{F}_{q^s}$ spanned by those roots is*

1. *If $\delta = 0$: of dimension $n - \min\{i \mid a_i \neq 0\}$. If $a_0 \neq 0$ then the smallest such field $\mathbb{F}_{q^s}$ is a difference splitting field (or Picard-Vessiot field) of $\mathcal{L}(Y) = 0$.*

2. *If $\delta \neq 0$: $n - \min\{i \mid \ell_i(a_0, \ldots, a_n, \beta) \neq 0\}$. If $\sum_{i=0}^n (-1)^i \beta^i a_i \neq 0$ then the smallest such field $\mathbb{F}_{q^s}$ is a δ-differential splitting field (or Picard-Vessiot field) of $\mathcal{L}(Y) = 0$.*

If $\mathbb{F}_{q^s}$ is a Picard-Vessiot field, then the elements of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ commute with θ and δ_θ and therefore in both cases send a solution into a solution. In this case we call $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ the Galois group of $\mathcal{L}(Y) = \sum_{i=0}^n a_i \mathcal{D}^i$.

For $\mathbb{F}_q[X; \theta, \delta_\beta]$ and $\sum_{i=0}^n (-1)^i \beta^i a_i \neq 0$ the solutions of the operator satisfy a polynomial over $\mathbb{F}_q$ and therefore all belong to a finite field extension of $\mathbb{F}_q$. The solution space is a vector space over the fixed field $(\mathbb{F}_q)^\theta$ of $\mathbb{F}_q$ which, in this case, contains the subfield of constants $\ker(\delta_\beta)$ since $\delta_\beta = \beta(\theta - id)$. If we denote $\mathbb{F}_{q^s}$ the field obtained by adjoining the solutions of $\mathcal{L}_f(y) = 0$, then $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ is the Galois group that transforms a solution of the operator into a solution (cf. [6], Theorem 1).

3 Skew evaluation codes

In this section we extend the notion of evaluation code introduced by E. Gabidulin in [8]. We will consider both the Hamming metric and the rank metric.

3.1 Definitions

Definition 8 *Let $n \in \mathbb{N}^*$ and $k \in \{1 \ldots, n\}$.*

- *Let $\underline{\alpha} = (\alpha_1, \ldots, \alpha_n) \in (\mathbb{F}_q)^n$ with $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) \geq k$. The* **remainder evaluation skew code** *of length n, dimension k and support $\underline{\alpha}$ is defined as*

$$\mathcal{C}_k(\alpha_1, \ldots, \alpha_n) = \{(f(\alpha_1), \ldots, f(\alpha_n)) \mid f \in \mathbb{F}_q[X; \theta, \delta], \deg(f) \leq k-1\}$$

- *Let $\underline{y} = (y_1, \ldots, y_n) \in (\mathbb{F}_q)^n$ with $\mathrm{rank}(\mathrm{Wr}_n^{\theta,\delta}(y_1, \ldots, y_n)) \geq k$ The* **operator evaluation skew code** *of length n, dimension k and support $\underline{y}$ is defined as*

$$\mathcal{C}_{k,\mathcal{L}}(y_1, \ldots, y_n) = \{(\mathcal{L}_f(y_1), \ldots, \mathcal{L}_f(y_n)) \mid f \in \mathbb{F}_q[X; \theta, \delta], \deg(f) \leq k-1\}$$

We now verify that the dimension of the codes defined above are k:
The generator matrix of $\mathcal{C}_k(\alpha_1, \ldots, \alpha_n)$ is

$$G_R^{\theta,\delta} = \begin{pmatrix} N_0^{\theta,\delta}(\alpha_1) & N_0^{\theta,\delta}(\alpha_2) & \cdots & N_0^{\theta,\delta}(\alpha_n) \\ N_1^{\theta,\delta}(\alpha_1) & N_1^{\theta,\delta}(\alpha_2) & \cdots & N_1^{\theta,\delta}(\alpha_n) \\ \vdots & \vdots & \cdots & \vdots \\ N_{k-1}^{\theta,\delta}(\alpha_1) & N_{k-1}^{\theta,\delta}(\alpha_2) & \cdots & N_{k-1}^{\theta,\delta}(\alpha_n) \end{pmatrix}$$

It coincides exactly with the rectangular Vandermonde matrix $V_{k,n}^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)$ ([11]) whose rank is $min(k, r)$ where r is the rank of $V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)$. Here $r \geq k$ so $\mathrm{rank}(G_R^{\theta,\delta}) = k$ and $\mathcal{C}_k(\alpha_1, \ldots, \alpha_n)$ is of dimension k.

The generator matrix of $\mathcal{C}_{k,\mathcal{L}}(y_1, \ldots, y_n)$ is

$$G_{\mathcal{L}}^{\theta,\delta} = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \mathcal{D}(y_n) \\ \vdots & \vdots & \cdots & \vdots \\ \mathcal{D}^{k-1}(y_1) & \mathcal{D}^{k-1}(y_2) & \cdots & \mathcal{D}^{k-1}(y_n) \end{pmatrix}$$

It coincides with the rectangular Wronskian matrix $\mathrm{Wr}_{k,n}^{\theta,\delta}(y_1, \ldots, y_n)$ whose rank is $min(k, r)$ where r is the dimension of the $(\mathbb{F}_q)^\theta$ space generated by $y_1, \ldots, y_n$. Here $r \geq k$ so $\mathrm{rank}(G_{\mathcal{L}}^{\theta,\delta}) = k$ and the code $\mathcal{C}_{k,\mathcal{L}}(y_1, \ldots, y_n)$ is of dimension k.

Note 3 *For $\delta = 0$ the operator evaluation $\mathcal{L}_f^\theta(y_1)$ coincides with the evaluation of the linearized polynomial. The corresponding operator evaluation codes are due to Gabidulin (cf. [8])*

3.2 Classification

Comparison of remainder evaluation skew codes with $\delta = 0$ and $\delta \neq 0$: The image of the relation $f = q \cdot (X - \alpha) + f(\alpha)$ in $\mathbb{F}_q[X; \theta, \delta]$ under the morphism (1) becomes

$$\mathcal{H}(f) \;=\; \mathcal{H}(q) \cdot (\, Z - \beta - \alpha) + f(\alpha)$$

in $\mathbb{F}_q[Z; \theta]$, showing that

$$f(\alpha) = \mathcal{H}(f)(\alpha + \beta) \tag{3}$$

Lemma 3 $\operatorname{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = \operatorname{rank}(V_n^{\theta}(\alpha_1 + \beta, \ldots, \alpha_n + \beta))$.

Proof: We first consider the case where all α_i are in the (θ, δ)-conjugacy class of $\alpha \in \mathbb{F}_q$.

- If $\alpha \neq -\beta$, we have $\operatorname{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = \dim_{\mathcal{C}^{\theta,\delta}(\alpha)}(y_1, \ldots, y_n)$, where y_i is defined by $\alpha_i = \alpha^{y_i}$. Furthermore $\alpha_i + \beta = \frac{\theta(y_i)}{y_i}\,\alpha + \frac{\delta(y_i)}{y_i} + \beta = \frac{\theta(y_i)}{y_i}\,(\alpha + \beta)$, so $\alpha_i + \beta = (\alpha + \beta)^{y_i}$ is θ-conjugated to $\alpha + \beta$, and we get

  $$\operatorname{rank}(V_n^{\theta}(\alpha_1 + \beta, \ldots, \alpha_n + \beta)) = \dim_{\mathcal{C}^{\theta}(\alpha+\beta)}(y_1, \ldots, y_n)$$

  Lastly $\mathcal{C}^{\theta,\delta}(\alpha) = (\mathbb{F}_q)^{\theta} = \mathcal{C}^{\theta}(\alpha + \beta)$ so $\operatorname{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = \operatorname{rank}(V_n^{\theta}(\alpha_1 + \beta, \ldots, \alpha_n + \beta))$.

- If $\alpha = -\beta$, then $\alpha_1 = \ldots = \alpha_n = -\beta$ and

  $$\operatorname{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = \operatorname{rank}(V_n^{\theta,\delta}(-\beta, \ldots, -\beta)) = 1.$$

  Since $\operatorname{rank}(V_n^{\theta}(\alpha_1 + \beta, \ldots, \alpha_n + \beta)) = \operatorname{rank}(V_n^{\theta}(0, \ldots, 0)) = 1$, we obtain the result.

If the α_i are not in the same (θ, δ)-conjugacy class, then $\{\alpha_1, \ldots, \alpha_n\}$ can be partitioned in distinct conjugacy classes $\{\alpha_1, \ldots, \alpha_n\} = A_1 \cup \cdots \cup A_r$. According to theorem 1, $\operatorname{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = \sum_{i=1}^{r} \operatorname{rank}(V^{\theta,\delta}(A_i))$. Considering $B_i = \{\alpha + \beta, \alpha \in A_i\}$, we have $\operatorname{rank}(V^{\theta,\delta}(A_i)) = \operatorname{rank}(V^{\theta}(B_i))$ and $\operatorname{rank}(V_n^{\theta}(\alpha_1 + \beta, \ldots, \alpha_n + \beta)) = \sum_{i=1}^{r} \operatorname{rank}(V^{\theta}(B_i))$, and the result follows. □

The above result shows that the map $\mathcal{H}$ is a linear isometry between the remainder evaluation skew codes of support $(\alpha_1, \ldots, \alpha_n)$, length n and dimension k (i.e with $\operatorname{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = k$) over $\mathbb{F}_q[X; \theta, \delta]$ and remainder evaluation skew code of support $(\alpha_1 + \beta, \ldots, \alpha_n + \beta)$, length n and dimension k (i.e $\operatorname{rank}(V_n^{\theta}(\alpha_1 + \beta, \ldots, \alpha_n + \beta)) = k$) over $\mathbb{F}_q[Z; \theta]$. Since H is constant on $\mathbb{F}_q$ the two codes are just two different constructions of the same codes. It is therefore sufficient to consider right remainder evaluation codes in $\mathbb{F}_q[X; \theta]$ (i.e. $\delta = 0$).

Comparison of remainder evaluation skew codes and operator evaluation skew codes with $\delta = 0$: If $\delta = 0$ and if $\operatorname{rank}(\operatorname{Wr}_n^{\theta}(y_1, \ldots, y_n)) = n$, the operator evaluation code of support $(y_1, \ldots, y_n)$ and dimension k over $\mathbb{F}_q[X; \theta]$ is the Gabidulin code of dimension k of support $y_1, \ldots, y_n$.

Let $f \in \mathbb{F}_q[X;\theta,\delta]$ and $0 \neq y_i \in \mathbb{F}_q$. Considering $\alpha_i = \frac{\mathcal{D}(y_i)}{y_i}$ we have $f(\alpha_i) = \frac{\mathcal{L}_f(y_i)}{y_i}$. Therefore (cf. [11] (4.12) page 325):

$$(\mathcal{L}_f(y_1),\ldots,\mathcal{L}_f(y_n)) = (f(\alpha_1),\ldots,f(\alpha_n)) \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & y_n \end{pmatrix}$$

This shows that operator evaluation codes whose support does not contain zero (which would correspond to a coordinate which is always zero) are always monomially equivalent to a remainder evaluation skew code. Note that the converse of the above does not hold since y_i may belong to a field extension of the field $\mathbb{F}_q$ containing the α_i, i.e. α_i may not be in the conjugacy class of 1.

Comparison of operator evaluation skew codes with $\delta = 0$ and with $\delta \neq 0$:

Lemma 4 *If $\delta \neq 0$, $\mathrm{rank}(\mathrm{Wr}_n^{\theta,\delta}(y_1,\ldots,y_n)) = n$ and $\exists u \in \mathbb{F}_q, \frac{\theta(u)}{u} = \beta$, then an operator evaluation code over $\mathbb{F}_q[X;\theta,\delta]$ is a Gabidulin code.*

Proof: Suppose that $\delta \neq 0$. For $\alpha_i = \frac{\delta(y_i)}{y_i}$,we have $\alpha_i + \beta = \beta\frac{\theta(y_i)}{y_i}$. Using (3), we obtain

$$(\mathcal{L}_f(y_1),\ldots,\mathcal{L}_f(y_n)) = (\mathcal{H}(f))(\alpha_1+\beta),\ldots,(\mathcal{H}(f))(\alpha_n+\beta)) \begin{pmatrix} y_1 & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & y_n \end{pmatrix}$$

If $\exists u \in \mathbb{F}_q, \frac{\theta(u)}{u} = \beta$, then a quick computation gives

$$(\mathcal{L}_f(y_1),\ldots,\mathcal{L}_f(y_n)) = u \times \left(\mathcal{L}_{\mathcal{H}(f)}(u\,y_1),\ldots,\mathcal{L}_{\mathcal{H}(f)}(u\,y_n)\right)$$

Furthermore $\mathrm{rank}(Wr_n^{\theta,\delta}(y_1,\ldots,y_n)) = \mathrm{rank}(Wr_n^{\theta}(u\,y_1,\ldots,u\,y_n))$ so we get two different constructions of the same operator evaluation code, up to the scalar multiplication by an element of $\mathbb{F}_q^*$. In particular the two codes have the same rank distance. According to [1] the Gabidulin codes of dimension k relatively to $(u\,y_1,\ldots,u\,y_n)$ and $(y_1,\ldots,y_n)$ are equal if $u \in \mathbb{F}_q^*$. □

3.3 MDS and MDR evaluation codes

We now give conditions for an evaluation code to be MDS (Maximum Distance Separable, for the Hamming metric) or MRD (Maximum Rank Distance, for the rank metric).

Proposition 2 *Let $n \in \mathbb{N}^*$, $y_i, \alpha_i \in \mathbb{F}_q, i = 1,\ldots,n$.*

1. *If* $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1,\ldots,\alpha_n)) = n$, *then the* remainder evaluation skew code *of length n, dimension k and support $(\alpha_1,\ldots,\alpha_n)$ is MDS.*

2. *If $y_1, \ldots, y_n$ are linearly independent over $(\mathbb{F}_q)^\theta$, then the* operator evaluation skew code *of length n, dimension k and of support $(y_1, \ldots, y_n)$ is MRD.*

Proof:

1. If a nonzero code word is of weight $< n-k+1$, then at least k coordinates, say the first k ones must vanish. This means that there exits a nonzero $f \in \mathbb{F}_q[X;\theta,\delta]$ of degree $< k$ such that $f(\alpha_i) = 0$ for $i \in \{1, \ldots, k\}$. The polynomial f is right divisible by $X - \alpha_i$ and therefore f is a right multiple of $\mathrm{lclm}(X-\alpha_1, \ldots, X-\alpha_k)$. Since $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = n$ implies that $\mathrm{rank}(V_k^{\theta,\delta}(\alpha_1, \ldots, \alpha_k)) = k$, we get from Theorem 2 that the degree of f is k. By assumption the degree of f is less than k, showing that a nonzero word of weight $< n-k+1$ cannot exist. This shows that the minimal distance of the code is $\geq n-k+1$ and we conclude using the "singleton bound".

2. The dual of a MRD code is MRD (cf. [8]), so let us consider the code with the test matrix $G_{\mathcal{L}}^{\theta,\delta}$ and let us prove that it is MRD by showing that it has no code word of rank $< k+1$ over $(\mathbb{F}_q)^\theta$. If c is a code word of rank $r < k+1$, then there exists $x = (x_1, \ldots, x_r)$ of rank r and a matrix M of size $r \times n$, rank r with coefficients in $(\mathbb{F}_q)^\theta$ such that $c = xM$. Then $G_{\mathcal{L}}^{\theta,\delta}\ c^T = G_{\mathcal{L}}^{\theta,\delta}\ M^T\ x^T = 0$ with $G_{\mathcal{L}}^{\theta,\delta} = \mathrm{Wr}_{k,n}^{\theta,\delta}(y_1, \ldots, y_n)$. As $r \leq k$, we get $\mathrm{Wr}_{r,n}^{\theta,\delta}(y_1, \ldots, y_n)\, M^T\ x^T = 0$. Let $(z_1, \ldots z_r)$ such that $(y_1, \ldots, y_n)\ M^T = (z_1, \ldots z_r)$, then as $\mathcal{D}$ is linear over $(\mathbb{F}_q)^\theta$ we get $\mathrm{Wr}_{r,n}^{\theta,\delta}(y_1, \ldots, y_n)\ M^T = \mathrm{Wr}_r^{\theta,\delta}(z_1, \ldots, z_r)$ and $\mathrm{Wr}_r^{\theta,\delta}(z_1, \ldots, z_r)\ x^T = 0$. Furthermore $z_1, \ldots, z_r$ are linearly independent over $(\mathbb{F}_q)^\theta$ because $y_1, \ldots, y_n$ are linearly independent over $(\mathbb{F}_q)^\theta$ and M has rank r so $\det(\mathrm{Wr}_r^{\theta,\delta}(z_1, \ldots, z_r)) \neq 0$, contradiction.

□

Note 4 *If $y_1, \ldots, y_n$ are linearly independent over $(\mathbb{F}_q)^\theta$ and if $\delta = 0$, then the* operator evaluation skew code *of support $(y_1, \ldots, y_n)$ is a MRD Gabidulin evaluation code ([8]). The condition $y_1, \ldots, y_n \in \mathbb{F}_q$ linearly independent over $(\mathbb{F}_q)^\theta$ implies that $n \leq [\mathbb{F}_q : (\mathbb{F}_q)^\theta]$. If $q = p^N$ with p prime number and if θ is the Frobenius automorphism, then $n \leq N$. The condition $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = n$ for $\alpha_1, \ldots, \alpha_n \in \mathbb{F}_q$ is less restrictive on the size of n. Let us consider $q = p^N$. Then there are p conjugacy classes : the conjugacy class of $-\beta$ and $p-1$ conjugacy classes each of size $\frac{p^N-1}{p-1}$. The rank of the Vandermonde matrix of elements lying in the same conjugacy class $\neq \{-\beta\}$ cannot be higher than $[\mathbb{F}_q : (\mathbb{F}_q)^\theta] = N$. So if $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = n$ then $n \leq (p-1)N+1$.*

Example 1 *Let $F = \mathbb{F}_{3^6} = \mathbb{F}_3(a)$ where $a^6 + 2\,a^4 + a^2 + 2\,a + 2 = 0$, $n = 13$, $k = 3$, $\beta = 1 \in F$, $\theta(u) = u^3$. Let $\underline{\alpha} = (2, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{14}, a^{25}) \in F^{13}$. We have $\mathrm{rank}(V_{13}(\underline{\alpha})) = 13$, so the remainder evaluation skew code of length 13, dimension $k < 13$ and support $\underline{\alpha}$ is a MDS code over $\mathbb{F}_{3^6}$. Notice that 13 is the maximal length of a remainder evaluation MDS code over $\mathbb{F}_{3^6}$ whereas 6 is the maximal length for an operator evaluation code over $\mathbb{F}_{3^6}$.*

4 Imposing a distance on skew module codes

In the following we consider the module (θ,δ)-code $(g)_{n,\theta,\delta}$ given in definition 1. We fix $\Delta \in \{0,\ldots,n\}$ and our aim is to construct $g \in \mathbb{F}_q[X;\theta,\delta]$ such that the minimal distance of the code is $\geq \Delta$. We will consider either the Hamming distance or the rank distance. Since the condition involves α_i belonging to an algebraic closure $\overline{\mathbb{F}_q}$ of $\mathbb{F}_q$, in the following we always extend any morphism $a \mapsto a^m$ to the morphism $a \mapsto a^m$ of the field extension $\mathbb{F}_q(\alpha_i) \subset \overline{\mathbb{F}_q}$.

Hamming condition 1 *: $\delta = 0$ and $\exists b \in \mathbb{N}$ and $\alpha \in \overline{\mathbb{F}_q}$ such that for $\alpha_i = \alpha^{i+b-1}$ ($1 \leq i \leq \Delta-1$) we have $g(\alpha_i) = 0$ $(1 \leq i \leq \Delta-1)$ and* $\mathrm{rank}(V_n^{id,0}(N_0^\theta(\alpha),\ldots,N_{n-1}^\theta(\alpha))) = n$.

Hamming condition 2 *: Let $b \in \mathbb{N}$ such that $b = 0$ if $\delta \neq 0$. There exists $\alpha \in \overline{\mathbb{F}_q}$ such that for $\alpha_i = N_{i+b-1}^{\theta,\delta}(\alpha)$ ($i = 1,\ldots,n$) we have $g(\alpha_i) = 0$ $(1 \leq i \leq \Delta-1)$,* $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1,\ldots,\alpha_n)) = n$ *and* $N_{i+b-1}^{\theta,\delta}(N_j^{\theta,\delta}(\alpha)) = N_j^{\theta,\delta}(N_{i+b-1}^{\theta,\delta}(\alpha)), i = 1,\ldots,\Delta-1, j = 0,\ldots,n-1$.

Rank condition 1 *: There exists a $y_1 \in \overline{\mathbb{F}_q}$ such that for $y_{i+1} = \mathcal{D}(y_i) = \mathcal{D}^i(y_1), i = 1,\ldots,n-1$ we have $\mathcal{L}_g(y_i) = 0, i = 1,\ldots,\Delta-1$ and* $\det(\mathrm{Wr}_n^{\theta,\delta}(y_1,\ldots,y_n)) \neq 0$.

Theorem 4 *1. If $g \in \mathbb{F}_q[X;\theta,\delta]$ satisfies the Hamming conditions 1 or 2, then the Hamming distance of the module skew code $(g)_{n,\theta,\delta}$ is $\geq \Delta$.*

2. If $g \in \mathbb{F}_q[X;\theta,\delta]$ satisfies the rank condition 1 then rank distance of the module skew code $(g)_{n,\theta,\delta}$ is $\geq \Delta$.

Proof:

1. We need to prove that the code has no nonzero word of Hamming weight $r < \Delta$. Such a word would be of the form $c = c_1X^{i_1} + c_2X^{i_2} + \cdots + c_rX^{i_r}$, where i_j are r distinct elements of $\{0,\ldots,n-1\}$ and $c_i \neq 0$. As a code word c is a right multiple of g and is therefore right divisible by $(X-\alpha_i)$, we get $c_1N_{i_1}^{\theta,\delta}(\alpha_i)+\cdots+c_rN_{i_r}^{\theta,\delta}(\alpha_i) = 0$. Therefore c is a nonzero element in the kernel of

$$H_r = \begin{pmatrix} N_{i_1}^{\theta,\delta}(\alpha_1) & \cdots & N_{i_{\Delta-2}}^{\theta,\delta}(\alpha_1) & N_{i_r}^{\theta,\delta}(\alpha_1) \\ N_{i_1}^{\theta,\delta}(\alpha_2) & \cdots & N_{i_{\Delta-2}}^{\theta,\delta}(\alpha_2) & N_{i_r}^{\theta,\delta}(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ N_{i_1}^{\theta,\delta}(\alpha_r) & \cdots & N_{i_{\Delta-2}}^{\theta,\delta}(\alpha_r) & N_{i_r}^{\theta,\delta}(\alpha_r) \end{pmatrix}. \quad (4)$$

In order to show that the minimum Hamming distance of the code is $\geq \Delta$, we need to insure that H_r is invertible when Hamming condition 1 or Hamming condition 2 is satisfied.

Hamming condition 1 Here $\delta = 0$, so $N_i^\theta(\alpha_j) = \left(N_i^\theta(\alpha)\right)^{j-1} \ \left(N_i^\theta(\alpha)\right)^b$ we obtain

$$H_r = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ N_{i_1}^\theta(\alpha) & N_{i_2}^\theta(\alpha) & \cdots & N_{i_r}^\theta(\alpha) \\ \vdots & \vdots & \vdots & \vdots \\ N_{i_1}^\theta(\alpha)^{\Delta-2} & N_{i_2}^\theta(\alpha)^{\Delta-2} & \cdots & (N_{i_r}^\theta(\alpha))^{\Delta-2} \end{pmatrix} \times \begin{pmatrix} N_{i_1}^\theta(\alpha)^b & 0 & \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & N_{i_r}^\theta(\alpha)^b \end{pmatrix}$$

So $\det(H_r) = \det(V_r^{id,0}(B)) \left(\prod_{j=1}^r N_{i_j}^\theta(\alpha)\right)^b$ where $B \subset \{N_0^\theta(\alpha), \ldots, N_{n-1}^\theta(\alpha)\}$. As $\mathrm{rank}(V_n^{id,0}(N_0^\theta(\alpha), \ldots, N_{n-1}^\theta(\alpha))) = n$, we get $\mathrm{rank}(V_r^{id,0}(B)) = r$ so $\det(H_r) \neq 0$ and $c = 0$.

Hamming condition 2 Let us assume that $b = 0$. Keeping the notation (4), we deduce from the relations

$$N_{i+b}^{\theta,\delta}(N_j^{\theta,\delta}(\alpha)) = N_j^{\theta,\delta}(N_{i+b}^{\theta,\delta}(\alpha)), i = 1, \ldots, \Delta - 1, j = 0, \ldots, n-1$$

that

$$H_r = \begin{pmatrix} N_0^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha)) & N_0^{\theta,\delta}(N_{i_2}^{\theta,\delta}(\alpha)) & \cdots & N_0^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha)) \\ N_1^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha)) & N_1^{\theta,\delta}(N_{i_2}^{\theta,\delta}(\alpha)) & \cdots & N_1^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha)) \\ \vdots & \vdots & \vdots & \vdots \\ N_{r-1}^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha)) & N_{r-1}^{\theta,\delta}(N_{i_2}^{\theta,\delta}(\alpha)) & \cdots & N_{r-1}^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha)) \end{pmatrix}$$

So $H_r = V_r^{\theta,\delta}(\alpha_{i_1+1}, \ldots, \alpha_{i_r+1})$. As $\{\alpha_{i_1+1}, \ldots, \alpha_{i_r+1}\}$ is a subset of $\{\alpha_1, \ldots, \alpha_n\}$ and $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = n$, we get $\det(H_r) \neq 0$ and $c = 0$.
If $b \neq 0$ and $\delta = 0$ then according to the proof of Proposition 2.9 (2) of [11], $N_{i+j}^{\theta,\delta}(\alpha) = N_j^{\theta,\delta}(\alpha)\, \theta^j(N_i^{\theta,\delta}(\alpha))$ so

$$H_r = \begin{pmatrix} N_b^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha))\theta^b(N_0^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha))) & \cdots & N_b^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha))\theta^b(N_0^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha))) \\ N_b^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha))\theta^b(N_1^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha))) & \cdots & \\ \vdots & \vdots & \vdots \\ N_b^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha))\theta^b(N_{r-1}^{\theta,\delta}(N_{i_1}^{\theta,\delta}(\alpha))) & \cdots & N_b^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha))\theta^b(N_{r-1}^{\theta,\delta}(N_{i_r}^{\theta,\delta}(\alpha))) \end{pmatrix}$$

$$\Rightarrow \ \det(H_r) = N_b^{\theta,\delta}\left(N_{i_1}^{\theta,\delta}(\alpha) \cdots N_{i_r}^{\theta,\delta}(\alpha)\right) \theta^b\left(\det\left(V_r^{\theta,0}(\alpha_{i_1+1}, \ldots, \alpha_{i_r+1})\right)\right) \neq 0$$

and $c = 0$.

2. We follow ideas of [8] to prove that the code has no nonzero word of rank $r < \Delta$. Consider a codeword $c \in (g)_{n,\theta,\delta}$ of rank $r \leq \Delta - 1$ over $(\mathbb{F}_q)^\theta$. Let $x = (x_1, \ldots, x_r)$ of rank r over $(\mathbb{F}_q)^\theta$ and M a $r \times n$ matrix with coefficients in $(\mathbb{F}_q)^\theta$ of rank r such that $c = xM$. As $c \in (g)_{n,\theta,\delta}$, there exists a $m \in \mathbb{F}_q[X; \theta, \delta]$ with degree $\leq k$ such

that $c(X) = m(X)g(X)$. According to Lemma 2, we have $\mathcal{L}_c(y_i) = \mathcal{L}_m(\mathcal{L}_g(y_i)) = 0$. So $H_r\ c^T = 0$ where

$$H_r = \begin{pmatrix} y_1 & \mathcal{D}(y_1) & \cdots & \mathcal{D}^{n-1}(y_1) \\ y_2 & \mathcal{D}(y_2) & \cdots & \mathcal{D}^{n-1}(y_2) \\ \vdots & & & \\ y_r & \mathcal{D}(y_r) & \cdots & \mathcal{D}^{n-1}(y_r) \end{pmatrix}$$

The vector x^T is a nonzero element in the kernel of $H_r\ M^T$ and we want to prove that $H_r\ M^T$ is invertible.

As $\mathcal{D}^{j-1}(y_i) = \mathcal{D}^{i-1}(y_j)$, we get :

$$H_r = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \mathcal{D}(y_n) \\ \vdots & & & \\ \mathcal{D}^{r-1}(y_1) & \mathcal{D}^{r-1}(y_2) & \cdots & \mathcal{D}^{r-1}(y_n) \end{pmatrix}$$

Let us define $(z_1, \ldots, z_r)$ such that $(y_1, y_2, \cdots, y_n)\ M^T = (z_1, \ldots, z_r)$. As $\mathcal{D}$ is linear over $(\mathbb{F}_q)^\theta$ we have :

$$H_r\ M^T = \begin{pmatrix} z_1 & z_2 & \cdots & z_r \\ \mathcal{D}(z_1) & \mathcal{D}(z_2) & \cdots & \mathcal{D}(z_r) \\ \vdots & & & \\ \mathcal{D}^{r-1}(z_1) & \mathcal{D}^{r-1}(z_2) & \cdots & \mathcal{D}^{r-1}(z_r) \end{pmatrix}$$

As $\dim_{(\mathbf{F}_q)^\theta}(y_1, \ldots, y_n) = n$ and $\mathrm{rank}(M) = r$, $z_1, \ldots, z_r$ are linearly independent over $(\mathbb{F}_q)^\theta$ so the determinant of the previous matrix is not zero, which contradicts $\mathrm{rank}(x) = r$.

□

Note that the rank condition 1 with $\delta = 0$ leads to Gabidulin codes. We are now going to refine the conditions given in the previous section to get MDS or MRD codes :

Theorem 5

- *If $g \in \mathbb{F}_q[X; \theta, \delta]$ satisfies the Hamming condition 1 or 2 with $\alpha \in \mathbb{F}_q$ and $g = \mathrm{lclm}(X - \alpha_i, i = 1, \ldots, n-k)$, then the code $(g)_{n,\theta,\delta}$ is MDS.*
- *If $g \in \mathbb{F}_q[X; \theta, \delta]$ satisfies the MRD condition 1 with $y_1 \in \mathbb{F}_q$ and $\mathcal{L}_g(y) = \mathrm{Wr}^{\theta,\delta}_{n-k+1}(y_1, \ldots, y_{n-k}, y)$, then the code $(g)_{n,\theta,\delta}$ is MRD.*

Proof: According to the hypothesis, $\deg(g) = n - k$, the code has a word of Hamming weight $\leq n-k+1$. So both the Hamming distance and the rank distance are $\leq n-k+1$. The remainder part of the proof follows directly from the theorem 4 with $\Delta = n-k+1$. □

Under certain conditions we get that the dual of $(g)_{n,\theta,\delta}$ is an evaluation skew code :

Proposition 3 *1. If* $(\alpha_1, \ldots, \alpha_n) \in \overline{\mathbb{F}_q}$ *and* $g \in \mathbb{F}_q[X; \theta, \delta]$ *satisfy the "Hamming condition 2" for* $\deg(g) = n - k$ *(i.e.* $g = lclm(X - \alpha_i, i \in \{1, \ldots, n-k\})$*, then the dual of module skew code* $(g)_{n,\theta,\delta}$ *is the remainder evaluation skew code of length* n*, dimension* $n - k$ *and support* $(\alpha_1, \ldots, \alpha_n)$*.*

2. If $(y_1, \ldots, y_n) \in \overline{\mathbb{F}_q}$ *and* $g \in \mathbb{F}_q[X; \theta, \delta]$ *satisfy the "rank condition1" for* $\deg(g) = n - k$ *(i.e.* $\mathcal{L}_g(Y) =\mid Wr^{\theta,\delta}(y_1, \ldots, y_{n-k}, Y) \mid$*), then the dual of module skew code* $(g)_{n,\theta,\delta}$ *is the operator evaluation skew code of length* n*, dimension* $n-k$ *and support* $(y_1, \ldots, y_n)$*.*

Proof:

1. The test matrix of the code is defined as

$$H = \begin{pmatrix} N_0^{\theta,\delta}(\alpha_1) & \cdots & N_{n-2}^{\theta,\delta}(\alpha_1) & N_{n-1}^{\theta,\delta}(\alpha_1) \\ N_0^{\theta,\delta}(\alpha_2) & \cdots & N_{n-2}^{\theta,\delta}(\alpha_2) & N_{n-1}^{\theta,\delta}(\alpha_2) \\ \vdots & \vdots & \vdots & \vdots \\ N_0^{\theta,\delta}(\alpha_{n-k}) & \cdots & N_{n-2}^{\theta,\delta}(\alpha_{n-k}) & N_{n-1}^{\theta,\delta}(\alpha_{n-k}) \end{pmatrix}$$

   As $N_{i-1}^{\theta,\delta}(N_j^{\theta,\delta}(\alpha)) = N_j^{\theta,\delta}(N_{i-1}^{\theta,\delta}(\alpha))$ $(i \in \{1, \ldots, n-k\}, j \in \{0, \ldots, n-1\})$ we get

$$H = \begin{pmatrix} N_0^{\theta,\delta}(\alpha_1) & \cdots & N_0^{\theta,\delta}(\alpha_{n-1}) & N_0^{\theta,\delta}(\alpha_n) \\ N_1^{\theta,\delta}(\alpha_1) & \cdots & N_1^{\theta,\delta}(\alpha_{n-1}) & N_1^{\theta,\delta}(\alpha_n) \\ \vdots & \vdots & \vdots & \vdots \\ N_{n-k-1}^{\theta,\delta}(\alpha_1) & \cdots & N_{n-k-1}^{\theta,\delta}(\alpha_{n-1}) & N_{n-k-1}^{\theta,\delta}(\alpha_n) \end{pmatrix}$$

   which is the generator matrix of the MDS remainder evaluation skew code of length n, dimension $n - k$ and support $(\alpha_1, \ldots, \alpha_n)$

2. Let $c \in (\mathbb{F}_q)^n$ be a code word. We have $\mathcal{L}_c(y_i) = 0$ for $i = 1, \ldots, \Delta - 1$ So $H\ c^T = 0$ where

$$H = \begin{pmatrix} y_1 & \mathcal{D}(y_1) & \cdots & \mathcal{D}^{n-1}(y_1) \\ y_2 & \mathcal{D}(y_2) & \cdots & \mathcal{D}^{n-1}(y_2) \\ \vdots & & & \\ y_{n-k} & \mathcal{D}(y_{n-k}) & \cdots & \mathcal{D}^{n-1}(y_{n-k}) \end{pmatrix} = \begin{pmatrix} y_1 & y_2 & \cdots & y_n \\ \mathcal{D}(y_1) & \mathcal{D}(y_2) & \cdots & \mathcal{D}(y_n) \\ \vdots & & & \\ \mathcal{D}^{n-k}(y_1) & \mathcal{D}^{n-k}(y_2) & \cdots & \mathcal{D}^{n-k}(y_n) \end{pmatrix}$$

   This is the generator matrix of the operator evaluation skew code of support $(y_1, \ldots, y_n)$, length n and dimension $n - k$.

□

Example 2 *Example over* $\mathbb{F}_{3^6} = \mathbb{F}_3(a)$*. Let* $\alpha = a$*,* $b = 0$ *and* $\beta = 0$*. The Hamming condition 2 is satisfied for* $n = 12$ *(Note that* $n = 12 > N = 6$*). The set* $\{N_i(\alpha), i \in \{0, \ldots, n-1\}\}$ *can be partitioned as* $\{a^{377}, a, a^{13}, a^{121}, a^{365}, a^{485}\} \cup \{a^{404}, 1, a^4, a^{40}, 2, a^{368}\}$ *such that the Vandermonde determinants of the two sets are not zero. For* $\Delta \leq 12$ *we have that* $g = \text{lclm}(X - N_i(\alpha), i = 1, \ldots, \Delta - 1) \in \mathbb{F}_{3^6}[X; \theta]$ *is of degree* $\Delta - 1$ *and generates a* $[n, n - \Delta + 1, \Delta]$ *skew code over* $\mathbb{F}_{3^6}$*:*

- *for $\Delta = 4$, we get $g = X^3 + 2X^2 + a^{12}x + a^{416}$ which generates $[4, 1, 4]$, $[5, 2, 4]$, $[6, 3, 4]$, $[7, 4, 4]$, $[8, 5, 4]$, ..., $[12, 9, 4]$ skew codes over $\mathbb{F}_{3^6}$.*
- *for $\Delta = 8$, then $g = X^7 + a^{401}X^6 + a^{680}X^5 + a^{18}X^4 + a^{32}X^3 + a^{477}X^2 + a^{725}x + a^{194}$ generates $[8, 1, 8]$, $[9, 2, 8]$, $[10, 3, 8]$, $[11, 4, 8]$ and $[12, 5, 8]$ skew codes over $\mathbb{F}_{3^6}$.*

5 Construction of BCH skew codes with prescribed distance over a given field $\mathbb{F}_q$

Most conditions to impose a distance in the previous sections deal with elements α_i or y_i in a field extension of $\mathbb{F}_q$. The goal of this section is to study how to start with such elements α_i in a field extension of $\mathbb{F}_q$ in order to obtain a code over $\mathbb{F}_q$. We start from α in a field extension of $\mathbb{F}_q$ and construct $g \in \mathbb{F}_q[X; \theta, \delta]$ of smallest degree such that $g(\alpha) = 0$. Repeating the procedure allows to construct codes for the Hamming conditions 1 and 2. For the rank condition 1 we start start from $y \neq 0$ in a field extension of $\mathbb{F}_q$ and construct $g \in \mathbb{F}_q[X; \theta, \delta]$ such that $\mathcal{L}_g(y) = 0$, but this is equivalent to construct g such that $g(\mathcal{D}(y)/y) = 0$ and therefore reduces to the previous problem.

Definition 9 *Let $\alpha \in \mathbb{F}_{q^s}$. The nonzero unitary polynomial f of minimal degree in $\mathbb{F}_q[X : \theta, \delta]$ such that $X - \alpha$ divides f on the right is called the* left skew (θ, δ)-minimal polynomial of α over $\mathbb{F}_q$ *and we will denote it* $\min_{\theta,\delta,q}(\alpha)$.

Proposition 4 *Let $\alpha \in \mathbb{F}_{q^s}$. Then*

$$\min_{\theta,\delta,q}(\alpha) = lclm\left\{X - \sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\right\},$$

where the computation of the lclm is performed in $\mathbb{F}_{q^s}[X; \theta, \delta]$ and θ denotes the extension of $\theta \in \mathrm{Aut}(\mathbb{F}_q)$ to $\mathrm{Aut}(\mathbb{F}_{q^s})$.

Proof: Form [14] we know that the lclm $lclm\left\{X - \sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\right\}$ exists and is unique. From Proposition 1, any $\tau \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ fixes $\beta \in \mathbb{F}_q$ and therefore gives an automorphism

$$\begin{array}{rcl} \varphi_\tau : \mathbb{F}_{q^s}[X; \theta, \delta] & \to & \mathbb{F}_{q^s}[X; \theta, \delta] \\ \sum_{i=0}^{n} a_i X^i & \mapsto & \sum_{i=0}^{n} \tau(a_i) X^i \end{array}$$

Therefore $\varphi_\tau(lclm\left\{X - \sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\right\})$ is right divisible by all $X - (\tau\sigma)(\alpha)$, where $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$. Since left multiplication (i.e. translation) by τ in $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ will permute the elements of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$, we obtain that the polynomial

$$\varphi_\tau(lclm\left\{X - \sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\right\})$$

is right divisible by all $X - \sigma(\alpha)$ for $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ comparing degrees, we see that $\forall \tau \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$

$$\varphi_\tau(lclm\left\{X - \sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\right\}) = lclm\left\{X - \sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\right\}.$$

This shows that the coefficients of $lclm\,\{X-\sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\}$ are fixed by any $\tau \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$ and therefore belong to $\mathbb{F}_q$, the fixed field of $\mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$.
In order to show that $lclm\,\{X-\sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\}$ is the left skew (θ,δ) minimal polynomial of α over $\mathbb{F}_q$, we note that if $f \in \mathbb{F}_q[X;\theta,\delta]$ is right divisible by $X-\alpha$ in $\mathbb{F}_{q^s}[X;\theta,\delta]$, then $f = q\cdot(X-\alpha)$ and using again the above automorphism φ_σ we get that $f = \varphi_\sigma(q)\cdot(X-\sigma(\alpha))$. This shows that f must be right divisible by all $X-\sigma(\alpha)$ for all $\sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)$, and therefore right divisible by $lclm\,\{X-\sigma(\alpha), \sigma \in \mathrm{Aut}(\mathbb{F}_{q^s}/\mathbb{F}_q)\}$. □

We note that if $[\mathbb{F}_p(\alpha):\mathbb{F}_p] = \ell$, then $\theta^\ell(\alpha) = 1$ showing that $X-\alpha$ and therefore $\min_{\theta,\delta,q}(\alpha)$ is a right divisor of $X^\ell - 1$. Also the polynomial $\min_{\theta,\delta,q}(\alpha)$ is not always irreducible over $\mathbb{F}_q[X;\theta]$. It may be explained by the following fact : if $\min_{\theta,\delta,q}(\alpha) = f\cdot g$, then either $g(\alpha) = 0$ or α is conjugated to a root of f (cf. [11] Theorem 2.7). So the polynomial g may not vanish at α. This is illustrated in the following example.

Example 3 *Let $F = \mathbb{F}_{3^6} = \mathbb{F}_3(a)$ and $\mathbb{F}_{3^2} = \mathbb{F}_3(b)$ where $b = a^{91}$. The polynomial $f = X^3+2\,X^2+2\,x+b^7$ is the minimal skew polynomial of a over $\mathbb{F}_{3^2}$. It is not irreducible over $\mathbb{F}_{3^2}$ as $f = (X+b)(X-b)(X-b^5)$ is a factorization of f in $\mathbb{F}_{3^2}[X;\theta]$. Furthermore $f(b^5) = 0$ but the minimal polynomial of b^5 is $X-b^5$ which divides f on the right. We also have $f(a^{321}) = 0$ and the minimal polynomial of a^{321} over $\mathbb{F}_{3^2}$ is $X^2+a^{182}X+a^{546} = X^2+b^2X+b^3$ which also divides f on the right : $(X+b)(X^2+b^2X+b^3) = f$.*

With the above, we can realize Hamming condition 1, 2 and rank condition 2 for a polynomial $g \in \mathbb{F}_q[X;\theta,\delta]$ of degree $\leq r$ and imposed distance Δ in the following way:

1. Select α in $\mathbb{F}_{q^r}$ where $r \leq \mid (\mathbb{F}_q)^\theta \mid^r$ and construct the α_i needed for the condition. Denote $\mathbb{F}_Q$ the field generated by adjoining the α_i to $\mathbb{F}_q$ and denote σ the generator of $\mathrm{Aut}(\mathbb{F}_Q/\mathbb{F}_q)$.

2. Compute the orbit S of $\{\alpha_i\}$ under σ. If $\mid S \mid \leq n$, then compute the skew polynomial $g = \mathrm{lclm}_{\gamma\in S}(X-\gamma) = lclm(min_{\theta,\delta,q}(\alpha_i), i = 1,\ldots,\Delta-1)$ and proceed. Otherwise start over with a new α.

3. If the α_i verify the corresponding rank condition(s), then a new code $(g)_{\theta,\delta}$ has been found.

For the rank condition 1 we need to construct the operator $\mathcal{L}(Y) \in \mathbb{F}_q[\mathcal{D};\circ]$ of smallest order such that a given set $y_1,\ldots,y_j$ belongs to the solution space of $\mathcal{L}(Y) = 0$. This can also be done either by constructing the corresponding operator directly, or using the above by constructing

$$g = \min_{\theta,\delta,q}\left(\frac{\mathcal{D}(y_1)}{y_1},\ldots,\frac{\mathcal{D}(y_{\Delta-1})}{y_j}\right)$$

and considering $\mathcal{L}_g(Y)$.

6 Decoding

6.1 Decoding remainder evaluation codes

For the rank distance, a Welch-Berlekamp like algorithm is presented in [13] to decode operator evaluation codes for $\delta = 0$. We now design a Welch-Berlekamp like algorithm to decode right remainder evaluation codes with the Hamming metric

Proposition 5 *Let $n \in \mathbb{N}^*$, $k \in \mathbb{N}^*$, $k < n$ and $\alpha_i \in \mathbb{F}_q$, $i \in 1, \ldots, n$ such that*

$$\text{rank}(V_n^{\theta,\delta}(\alpha_1, \ldots, \alpha_n)) = n.$$

Consider the right remainder evaluation code

$$\mathcal{C}_k(\alpha_1, \ldots, \alpha_n) = \{(f(\alpha_1), \ldots, f(\alpha_n))/f \in \mathbb{F}_q[X; \theta, \delta], \deg(f) \leq k-1\}$$

If for $c \in \mathcal{C}_k(\alpha_1, \ldots, \alpha_n)$ and $v \in (\mathbb{F}_q)^n$ the weight of $v - c$ is $\leq t = (n-k-1)/2$, then for $Q_0, Q_1 \in \mathbb{F}_q[X; \theta, \delta]$ such that

- $\deg(Q_0) \leq k + t$ *and* $\deg(Q_1) \leq t$
- $\forall i \in \{1, \ldots, n\}, Q_0(\alpha_i) + Q_1(\alpha_i^{v_i})v_i = 0$ *if* $v_i \neq 0$, $Q_0(\alpha_i) = 0$ *if* $v_i = 0$

we can recover c as $(f(\alpha_1), \ldots, f(\alpha_n))$, where f is the quotient in the left division of Q_0 by $-Q_1$ in $\mathbb{F}_q[X; \theta, \delta]$.

Proof: Let c be a code word and $v \in (\mathbb{F}_q)^n$ such that $w(v-c) \leq t = (n-k-1)/2$. Since the minimum distance of the code is $n-k+1$, c is the unique code word such that $w(v-c) \leq t$. Let $f \in \mathbb{F}_q[X; \theta, \delta]$ with $\deg(f) \leq k-1$ such that $c = (f(\alpha_1), \ldots, f(\alpha_n))$. Let R defined by $R = Q_0 + Q_1 \cdot f$ where $\deg(Q_0) \leq k+t$, $\deg(Q_1) \leq t$ and the coefficients of Q_0, Q_1 satisfy the linear system given by

$$\begin{array}{rrcl} \forall i \in \{1, \ldots, n\}, & Q_0(\alpha_i) + Q_1(\alpha_i^{v_i})v_i & = & 0 \quad \text{if } v_i \neq 0 \\ & Q_0(\alpha_i) & = & 0 \quad \text{if } v_i = 0 \end{array}$$

Our goal is to prove that $R = 0$, which then allows to compute f as the quotient in the left division of Q_0 by $-Q_1$ in $\mathbb{F}_q[X; \theta, \delta]$ and to reconstruct c.
Let us evaluate R at α_i. According to Product Theorem 2.7 of [11], we have,

$$\begin{array}{rcll} \forall i \in \{1, \ldots, n\}, R(\alpha_i) & = & Q_0(\alpha_i) + Q_1(\alpha_i^{c_i})c_i & \text{if } c_i \neq 0 \\ & = & Q_0(\alpha_i) & \text{if } c_i = 0 \end{array}$$

As $w(v-c) \leq t$, there are at least $n-t$ positions i (without lost of generality, say $1, 2, \ldots, n-t$) such that $v_i = c_i$, so

$$\begin{array}{rcll} \forall i \in \{1, \ldots, n-t\}, R(\alpha_i) & = & Q_0(\alpha_i) + Q_1(\alpha_i^{v_i})v_i & \text{if } v_i \neq 0 \\ & = & Q_0(\alpha_i) & \text{if } v_i = 0 \end{array}$$

So according to the hypothesis on Q_0 and Q_1, we get $R(\alpha_i) = 0$ for all $i \in \{1, \ldots, n-t\}$ which implies that R is right divisible by $\text{lclm}(X - \alpha_i, i = 1, .., n-t)$. If $R \neq 0$, then, as

$\mathrm{rank}(V_{n-t}^{\theta,\delta}(\alpha_1,\ldots,\alpha_{n-t})) = n-t$, the polynomial R is of degree at least $n-t=(n+k)/2$. Since by construction R is of degree at most $k+t=(n+k)/2$, we must have $R=0$. $\square$

This leads to the following decoding algorithm for a MDS remainder evaluation skew code of length n, dimension k and support $(\alpha_1,\ldots,\alpha_n)$ satisfying $\mathrm{rank}(V_n^{\theta,\delta}(\alpha_1,\ldots,\alpha_n)) = n$:

Input : $v \in (\mathbb{F}_q)^n$ such that $v = c + e$ with $w(e) \leq t = (n-k-1)/2$ and c a code word
Output: c
1. Construct the system (S) with $n+1$ unknowns and n equations given by

$$(S)\ \begin{cases} \text{if } v_i = 0: & \sum_{j=0}^{k+t} q_j\, N_j(\alpha_i) = 0 \\ \text{if } v_i \neq 0: & \sum_{j=0}^{k+t} q_j\, N_j(\alpha_i) + \sum_{j=0}^{t} q_{k+t+j+1}\, N_j(\theta(v_i)/v_i\,(\alpha_i+\beta)-\beta)\, v_i = 0 \end{cases}$$

and compute a solution $q_0,\ldots q_n$ of (S)
2. Compute the quotient f in the left division of $Q_0(X)$ by $-Q_1(X)$ in $\mathbb{F}_q[X;\theta,\delta]$, where $Q_0(X) := \sum_{j=0}^{k+t} q_j X^j$ and $Q_1(X) := \sum_{j=0}^{t} q_{j+1+k+t} X^j$
3. Return $c = (f(\alpha_1),\ldots,f(\alpha_n))$

Example 4 *Consider* $\mathbb{F}_{3^6} = \mathbb{F}_3(a)$ *where* $a^6 + 2\,a^4 + a^2 + 2\,a + 2 = 0$.

- *Consider the ring in* $\mathbb{F}_{3^6}[X;\theta]$ *(*$\delta = 0$*) and* $\underline{\alpha} = (a, a^2, a^3, a^4, a^5, a^7)$. *Since* $\mathrm{rank}(V(\underline{\alpha})) = 6$, *the skew remainder evaluation code of support* $\underline{\alpha}$ *is an MDS* $[6,3,4]$ *code over* $\mathbb{F}_{3^6}$. *For* $f = X^2 + X + a \in \mathbb{F}_{3^6}[X;\theta]$ *we consider the received word*

$$v = (f(\alpha_1),\ldots,f(\alpha_5), a^{341}) = (a^9, a^{357}, a^{257}, a^{727}, a^{34}, a^{341}).$$

  Since $f(\alpha_6) \neq a^{341}$ *this received word contains one error which we now correct by recovering* f *:*

  1. *the matrix of the system* (S) *is the* 6×7 *matrix*

$$\begin{pmatrix} 1 & a & a^4 & a^{13} & a^{40} & a^9 & a^{28} \\ 1 & a^2 & a^8 & a^{26} & a^{80} & a^{357} & a^{345} \\ 1 & a^3 & a^{12} & a^{39} & a^{120} & a^{257} & a^{46} \\ 1 & a^4 & a^{16} & a^{52} & a^{160} & a^{727} & a \\ 1 & a^5 & a^{20} & a^{65} & a^{200} & a^{34} & a^{107} \\ 1 & a^7 & a^{28} & a^{91} & a^{280} & a^{341} & a^{302} \end{pmatrix}$$

  2. *its kernel is generated by* $(1, a^{370}, a^{328}, a^{184}, 0, a^{363}, a^{548})$.
  3. *We obtain* $Q_0 = a^{184}X^3 + a^{328}X^2 + a^{370}X + 1$ *and* $Q_1 = a^{548}X + a^{363}$
  4. *The left quotient of* Q_0 *by* $-Q_1$ *in* $\mathbb{F}_{3^6}[X;\theta]$ *is* $f = X^2 + X + a$

- *Consider the ring* $\mathbb{F}_{3^6}[X;\theta,\delta_1]$ *and* $\underline{\alpha} = (2, a, a^2, a^3, a^4, a^5, a^6, a^7, a^8, a^9, a^{10}, a^{14}, a^{25})$. *Since* $\mathrm{rank}(V(\underline{\alpha})) = 13$, *the skew remainder evaluation code of support* $\underline{\alpha}$ *is an MDS* $[13,6,8]$ *code over* $\mathbb{F}_{3^6}$. *For* $f = X^5 + aX^2 + X + a \in \mathbb{F}_{3^6}[X;\theta,\delta_1]$ *we consider the received word* $v = (f(\alpha_1),\ldots,f(\alpha_{10}), a^{708}, a^{487}, a^{183})$ *given by*

$$v = (a^{221}, a^{464}, a^{180}, a^{416}, a^{720}, a^{261}, a^{400}, a^{201}, a^{218}, a^{708}, a^{487}, a^{183}).$$

Since $f(\alpha_j) \neq v_j$ for $11 \leq j \leq 13$, such a received word contains three errors which we now correct by recovering f :

1. *the matrix of the system (S) is a 13×14 matrix*
2. *its kernel is generated by*

$$(1, a^{335}, a^{707}, a^{157}, a^{112}, a^{198}, a^{632}, a^{587}, a^{490}, 0, 1, a^{268}, a^{223}, a^{126})$$

3. *this yields the polynomials $Q_0 = a^{490}X^8 + a^{587}X^7 + a^{632}X^6 + a^{198}X^5 + a^{112}X^4 + a^{157}X^3 + a^{707}X^2 + a^{335}x + 1$ and $Q_1 = a^{126}X^3 + a^{223}X^2 + a^{268}x + 1$*
4. *The left quotient of Q_0 by $-Q_1$ in $\mathbb{F}_{3^6}[X; \theta, \delta_1]$ is $f = X^5 + aX^2 + X + a$*

6.2 Decoding module codes

6.2.1 Hamming condition 1

Recall that under this condition$\delta = 0$. A decoding algorithm for this condition based on Euclid's algorithm can be found in [2] and [6], we present here a slightly different method. For the presentation we will assume that $b = 0$ and $\Delta = 2t + 1$.

Consider $g \in \mathbb{F}_q[X; \theta]$ and $\alpha \in \overline{\mathbb{F}_q}$ such that for $\alpha_i = \alpha^{i+b-1}$ $(1 \leq i \leq \Delta - 1)$ we have $g(\alpha_i) = 0$ $(1 \leq i \leq \Delta - 1)$ and $\text{rank}(V_n^{id,0}(N_0^\theta(\alpha), \ldots, N_{n-1}^\theta(\alpha)) = n$.

Let c be a code word in $(g)_{n,\theta}$ and $e = \sum_{j=1}^r e_j X^{i_j} \in \mathbb{F}_q[X; \theta]$ with $e_j \neq 0$, $r \leq t$ and $0 \leq i_1 < i_2 < \cdots < i_r \leq n - 1$ an error of Hamming weight t. For a received word $v = c + e$ we obtain at $\alpha_j = N_{i_j}(\alpha)$ the syndrome

$$S_i = e(\alpha^{i-1}) = \sum_{j=1}^r e_j \, N_{i_j}(\alpha^{i-1}) = \sum_{j=1}^r e_j \, N_{i_j}(\alpha)^{i-1} = \sum_{j=1}^r e_j \, \alpha_j^{i-1}$$

We consider a commutative error localizator polynomial with unknown coefficients :

$$h = (Z - \alpha_1) \cdots (Z - \alpha_r) = Z^r + \sum_{j=1}^r h_j Z^{j-1} \in \mathbb{F}_q[Z]$$

From $h(\alpha_i) = 0, (Z \cdot h)(\alpha_i) = 0, \ldots, (Z^{r-1} \cdot h)(\alpha_i) = 0$, for $i \in \{1, \ldots, r\}$ we obtain:

$$\left\{ \begin{array}{lcl} \alpha_i^r + \sum_{j=1}^r h_j \alpha_i^{j-1} & = & 0 \\ \alpha_i^{r+1} + \sum_{j=1}^r h_j \alpha_i^{j-1} & = & 0 \\ \vdots & & \\ \alpha_i^{2r-1} + \sum_{j=1}^r h_j \alpha_i^{j+r-2} & = & 0 \end{array} \right.$$

Multiplying the first equation by e_i for $i \in \{1, \ldots r\}$ we get $e_i \, \alpha_i^r + \sum_{j=1}^r h_j e_i \, \alpha_i^{j-1} = 0$. If we sum on i we obtain $S_{r+1} + \sum_{j=1}^r h_j S_j = 0$. Repeating the same trick for the $2r - 1$ other equations we get

$$\left\{ \begin{array}{lcl} S_{r+1} + \sum_{j=1}^r h_j S_j & = & 0 \\ S_{r+2} + \sum_{j=1}^r h_j S_{j+1} & = & 0 \\ \vdots & & \\ S_{2r} + \sum_{j=1}^r h_j S_{r+j-1} & = & 0 \end{array} \right. , \quad \text{corresponding to} \quad \mathcal{S} \left(\begin{array}{c} h_1 \\ h_2 \\ \vdots \\ h_r \end{array} \right) = b \qquad (5)$$

where

$$\mathcal{S} = \begin{pmatrix} S_1 & S_2 & \cdots & \cdots & S_r \\ S_2 & S_3 & \cdots & \cdots & S_{r+1} \\ & & & & \\ & & & & \\ S_r & & & & S_{2r} \end{pmatrix} \quad \text{and} \quad b = \begin{pmatrix} -S_{r+1} \\ \vdots \\ \vdots \\ -S_{2r} \end{pmatrix}$$

A quick computation gives $\mathcal{S} = VDV^T$, where D is a diagonal matrix with $e_1\alpha_1 \dots e_r\alpha_r$ on its diagonal and $V = V_n^{id,0}(\alpha_1, \dots, \alpha_r)$ whose rank is r according to the definition of the code above. The matrix $\mathcal{S}$ is invertible and we can compute the coefficients of h as solution of the linear system above and then find the positions of the errors thanks to the zeroes of h. Here is the corresponding algorithm :

Input : $v = c + e$ with $\mathrm{w}(e) = r \leq t$ and c word of a code satisfying Hamming Condition 1
Output : c

1. Compute S_i for $i = 1, \dots, 2t$ and the matrix $\mathcal{S}$ above for $r = t$.
2. While $\det(\mathcal{S}) = 0$ do $r := r - 1$; compute $\mathcal{S}$; end while
3. Compute the solution $(h_1, \dots, h_r)$ of the linear system given by (5)
4. Find $i_1, \dots, i_r$ such that $h(N_{i_j}(\alpha)) = 0$ where $h = Z^r + \sum_{i=1}^r h_i Z^{i-1} \in \mathbb{F}_q[Z]$
5. Compute $e_1, \dots, e_r$ given by the r equations $S_i = \sum_{j=1}^{r} e_j\, \alpha_j^{i-1}$ where $\alpha_j = N_{i_j}(\alpha)$
6. Return $c = v - \sum_{j=1}^r e_j X^{i_j}$

6.2.2 Rank condition 1

We follow Gabidulin's decoding algorithm ([9]) for $\mathbb{F}_q[X;\theta]$ which we extend to module codes $(g)_{n,\theta,\delta}$ over $\mathbb{F}_q[X;\theta,\delta]$. Suppose that for $g \in \mathbb{F}_q[X;\theta]$ there exists $y = y_1 \in \overline{\mathbb{F}_q}$ such that for $y_{i+1} = \mathcal{D}(y_i) = \mathcal{D}^i(y), i = 1, \dots, n-1$ we have $\mathcal{L}_g(y_i) = 0, i = 1, \dots, \Delta - 1$ and $\det(\mathrm{Wr}_n^{\theta,\delta}(y_1, \dots, y_n)) \neq 0$.

Let c be a code word and $e = (e_0, \dots, e_{n-1}) \in (\mathbb{F}_q)^n$ with rank $r \leq t = (\Delta - 1)/2$. If the received word is $v = c + e$ and we want to recover c from v. Let us define the syndrome $S_j = \mathcal{L}_v(y_j)$. By construction, we have $S_j = \mathcal{L}_c(y_j) + \mathcal{L}_e(y_j) = \mathcal{L}_e(y_j), j = 1, \dots, 2t$. Consider $x \in (\mathbb{F}_q)^r$ with $\mathrm{rank}(x) = r$ and $M \in \mathcal{M}((\mathbb{F}_q)^\theta, r, n)$ of rank r such that $e = xM$. Our aim is to construct a polynomial of degree r whose space of solutions enables to recover x and then M. For $j \in \{1, \dots, 2t\}$ we obtain

$$S_j = \sum_{i=0}^{n-1} e_i\, \mathcal{D}^i(\mathcal{D}^{j-1}(y)) = \sum_{i=0}^{n-1} \left(\sum_{l=1}^{r} x_l M_{l,i+1} \right) \mathcal{D}^i(\mathcal{D}^{j-1}(y))$$

$$= \sum_{l=1}^{r} x_l \sum_{i=0}^{n-1} M_{l,i+1} \mathcal{D}^{j-1}(\mathcal{D}^i(y)) = \sum_{l=1}^{r} x_l \mathcal{D}^{j-1} \left(\underbrace{\sum_{i=0}^{n-1} M_{l,i+1} \mathcal{D}^i(y)}_{z_l} \right) = \sum_{l=1}^{r} x_l \mathcal{D}^{j-1}(z_l)$$

where the $z_1, \ldots, z_r$ are defined by the relation $M(y_1, \ldots, y_n)^T = (z_1, \ldots, z_r)^T$. Since $y_1, \ldots, y_n$ are linearly independent over $(\mathbb{F}_q)^\theta$ and M is a rank r matrix over $(\mathbb{F}_q)^\theta$, we also have that $z_1, \ldots, z_r$ are linearly independent over $(\mathbb{F}_q)^\theta$. Once we computed the z_i, we can recover x_l from the the linear system $S_j = \sum_{l=1}^{r} x_l \mathcal{D}^{j-1}(z_l)$.

To find the z_l we are going to construct the polynomial $h = \sum_{i=0}^{r} h_i x^i \in \mathbb{F}_q[X; \theta, \delta]$ with $h_r = 1$ such that the space of solutions of $\mathcal{L}_h$ is generated by $z_1, \ldots, z_r$. The coefficients of this polynomial will satisfy a linear system depending on the S_i. We first derive one equation of this linear system and will explain later how to find the remaining $r-1$ equations. For $l \in \{1, \ldots, r\}$ we have

$$\mathcal{L}_h(z_l) = \sum_{j=1}^{r+1} h_{j-1} \mathcal{D}^{j-1}(z_l) = 0 \tag{6}$$

Multiplying each equation by x_l, we get $\sum_{j=1}^{r+1} h_{j-1} x_l \mathcal{D}^{j-1}(z_l) = 0$ ($l \in \{1, \ldots, r\}$). Summing these equations over $l = 1, \ldots, r$, we get a linear relation between h_l given by $\sum_{j=1}^{r+1} h_{j-1} S_j = 0$.

In order to get the $r-1$ other linear relations between the coefficients of h we follow the same idea as in [9] : applying θ^{i-1} to (6) for $i = 2, \ldots, r$ we have

$$\theta^{i-1}(\mathcal{L}_h(z_l)) = \sum_{j=1}^{r+1} \theta^{i-1}(h_{j-1}) \theta^{i-1}\left(\mathcal{D}^{j-1}(z_l)\right) = 0, l = 1, \ldots, r \tag{7}$$

If $\beta = 0$ (the case considered in [9]), then $\mathcal{D} = \theta$ and $\theta^{i-1}(\mathcal{D}^{j-1}(z_l)) = \theta^{i+j-2}(z_l)$. Multiplying each equation of (7) by x_l and summing all the equations over $l \in \{1, \ldots, r\}$ one gets the $r-1$ other linear equations in $h_0, \ldots, h_{r-1}, h_r = 1$:

$$\sum_{j=1}^{r+1} \theta^{i-1}(h_{j-1}) S_{i+j-1} = 0$$

If $\beta \neq 0$, the idea is to express $\theta^{i-1}(\mathcal{D}^{j-1}(z_l))$ as a sum of $\mathcal{D}^m(z_l)$ whose coefficients depend only on β using the following lemma:

Lemma 5 *Consider $i \in \mathbb{N}^*$ and $u \in \mathbb{F}_q$. Then $\theta^{i-1}(u)$ can be written as $\theta^{i-1}(u) = \sum_{k=1}^{i} a_{i,k}(\beta) \mathcal{D}^{k-1}(u)$ where the coefficients $a_{i,j}(\beta)$ are defined by :*

- *if $\beta \neq 0$: $a_{1,1}(\beta) = 1$, $a_{1,j}(\beta) = 0$ ($j \geq 2$) and $a_{i+1,j+1}(\beta) = \frac{1}{\beta}\theta(a_{i,j}(\beta)) + \theta(a_{i,j+1}(\beta))$.*
- *if $\beta = 0$: $a_{i,i}(0) = 1$ and $a_{i,j}(0) = 0$ for $i \neq j$.*

Proof: For $\beta \neq 0$, we proceed by induction on i. We have $\theta^0(u) = u = a_{1,1}\mathcal{D}^0(u)$. Consider $i \geq 1$ such that $\theta^{i-1}(u) = \sum_{k=1}^{i} a_{i,k}(\beta)\mathcal{D}^{k-1}(u)$. Then $\theta^i(u) = \sum_{k=1}^{i} \theta(a_{i,k}(\beta))\theta(\mathcal{D}^{k-1}(u))$. As $\theta = 1/\beta\delta + id$, we get

$$\begin{aligned} \theta^i(u) &= \sum_{k=1}^{i} \theta(a_{i,k}(\beta))(1/\beta\mathcal{D}^k(u) + \mathcal{D}^{k-1}(u)) \\ &= \sum_{k=1}^{i+1} (1/\beta\theta(a_{i,k-1}(\beta)) + \theta(a_{i,k}(\beta)))\mathcal{D}^{k-1}(u)) \end{aligned}$$

As $a_{i+1,k-1}(\beta) = 1/\beta\theta(a_{i,k-1}(\beta)) + \theta(a_{i,k}(\beta))$, we get the result. □

The lemma below describes how to construct the polynomial h in the case where $\beta \in \mathbb{F}_q$.

Lemma 6 *Consider* $h = X^r + \sum_{i=0}^{r-1} h_i X^i \in \mathbb{F}_q[X;\theta,\delta]$ *such that* $\mathcal{L}_h(z_i) = 0$

1. *The coefficients* $h_0, \ldots, h_{r-1}$ *satisfy the linear system :*$\mathcal{S} \cdot (h_0, h_1, \ldots, h_{r-1})^T = b$, *where*

$$\mathcal{S}_{i,j} = \theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta) S_{k+j-1}\right), \quad b_i = -\theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta) S_{k+r}\right)$$

and $a_{i,j}(\beta)$ *are defined by :*

- *if* $\beta \neq 0$ *:* $a_{1,1}(\beta) = 1$, $a_{1,j}(\beta) = 0$ *(*$j \geq 2$*) and* $a_{i+1,j+1}(\beta) = \frac{1}{\beta}\theta(a_{i,j}(\beta)) + \theta(a_{i,j+1}(\beta))$.
- *if* $\beta = 0$ $a_{i,i}(0) = 1$ *and* $a_{i,j}(0) = 0$ *for* $i \neq j$.

2. *The matrix* $\mathcal{S}$ *is an invertible matrix satisfying the relation :*

$$\mathcal{S} = \begin{pmatrix} x_1 & \cdots & \cdots & x_r \\ \theta^{-1}(x_1) & \cdots & \cdots & \theta^{-1}(x_r) \\ \\ \theta^{1-r}(x_1) & \cdots & \cdots & \theta^{1-r}(x_r) \end{pmatrix} \times \begin{pmatrix} z_1 & \cdots & \cdots & \mathcal{D}^{r-1}(z_1) \\ z_2 & \cdots & \cdots & \mathcal{D}^{r-1}(z_2) \\ \\ z_r & \cdots & \cdots & \mathcal{D}^{r-1}(z_r) \end{pmatrix}$$

Proof:

1. Let $i \in \{1, \ldots, r\}$. According to (7)

$$\sum_{j=1}^{r+1} \theta^{i-1}(h_{j-1}) \theta^{i-1}\left(\mathcal{D}^{j-1}(z_l)\right) = 0, l = 1, \ldots, r$$

Applying lemma 5 to $\theta^{i-1}\left(\mathcal{D}^{j-1}(z_l)\right)$ we obtain

$$\sum_{j=1}^{r+1} \theta^{i-1}(h_{j-1}) \sum_{k=1}^{i} a_{i,k}(\beta) \mathcal{D}^{k-1}(\mathcal{D}^{j-1}(z_l)) = 0, l = 1, \ldots, r$$

For each l we multiply this equation by x_l and sum the r equations over l, we get

$$\sum_{j=1}^{r+1} \theta^{i-1}(h_{j-1}) \sum_{k=1}^{i} a_{i,k}(\beta) S_{k+j-1} = 0$$

$$\Rightarrow \quad \sum_{j=1}^{r} \theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta) S_{k+j-1}\right) \; h_{j-1} = -\theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta) S_{k+r}\right)$$

2. Let us prove that $\mathcal{S}$ is invertible.

$$\begin{aligned}
\mathcal{S}_{i,j} &= \theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta) S_{k+j-1}\right) \\
&= \sum_{k=1}^{i} \theta^{-i+1}\left(a_{i,k}(\beta)\right)\theta^{-i+1}\left(\sum_{l=1}^{r} x_l \mathcal{D}^{k+j-2}(z_l)\right) \\
&= \sum_{l=1}^{r} \theta^{-i+1}(x_l)\theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta)\mathcal{D}^{k+j-2}(z_l)\right) \\
&= \sum_{l=1}^{r} \theta^{-i+1}(x_l)\theta^{-i+1}\left(\sum_{k=1}^{i} a_{i,k}(\beta)\mathcal{D}^{k-1}(\mathcal{D}^{j-1}(z_l))\right) \\
&= \sum_{l=1}^{r} \theta^{-i+1}(x_l)\theta^{-i+1}\left(\theta^{i-1}(\mathcal{D}^{j-1}(z_l))\right) \\
&= \sum_{l=1}^{r} \theta^{-i+1}(x_l)\mathcal{D}^{j-1}(z_l)
\end{aligned}$$

$$\Rightarrow \mathcal{S} = \begin{pmatrix} x_1 & \cdots & \cdots & x_r \\ \theta^{-1}(x_1) & \cdots & \cdots & \theta^{-1}(x_r) \\ & & & \\ \theta^{1-r}(x_1) & \cdots & \cdots & \theta^{1-r}(x_r) \end{pmatrix} \times \begin{pmatrix} z_1 & \cdots & \cdots & \mathcal{D}^{r-1}(z_1) \\ z_2 & \cdots & \cdots & \mathcal{D}^{r-1}(z_2) \\ & & & \\ z_r & \cdots & \cdots & \mathcal{D}^{r-1}(z_r) \end{pmatrix}$$

so $\mathcal{S}$ is invertible.

□

We deduce from this the following algorithm :

Input : $v = c + e$ with $\text{rank}(e) = r \leq t$ and c word of a code satisfying rank condition 1
Output : c

1. Compute S_i for $i = 1, \ldots, 2t$ and the matrix $\mathcal{S}$ given in lemma 6, point 1 with $r = t$
2. While $\det(\mathcal{S}) = 0$ do $r := r - 1$; compute $\mathcal{S}$; end while
3. Compute the solution $(h_1, \ldots, h_r)$ of the linear system given in lemma 6
4. Compute a basis of solutions $z_1, \ldots, z_r$ of $\mathcal{L}_h$ over $\mathbb{F}_q^\theta$ where $h = X^r + \sum_{i=1}^{r} h_i X^{i-1}$
5. Construct $x = (x_1, ..., x_r)$ as a solution of $S_j = \sum_{l=1}^{r} x_l \mathcal{D}^{j-1}(z_l), j = 1, \ldots, r$
6. Construct $M \in \mathcal{M}(\mathbb{F}_q^\theta, r, n)$ such that $M(y_1, \ldots, y_n)^T = (z_1, \ldots, z_r)^T$
7. Construct $e = xM$ and $c = v - e$

7 Acknowledgements

We thank Michael Singer for many discussions and useful suggestions.

References

[1] T. Berger *Isometries for Rank Distance and Permutation Group of Gabidulin Codes.* IEEE Transactions on Information Theory, Vol 49, No. 11 (2003)

[2] D. Boucher, W. Geiselmann and F. Ulmer, *Skew Cyclic Codes*, Applied Algebra in Engineering, Communication and Computing, Volume 18, Number 4, p. 379-389 (2007)

[3] D. Boucher and F. Ulmer, *Coding with skew polynomial rings*, Journal of Symbolic Computation, 44, 1644-1656 (2009)

[4] D. Boucher and F. Ulmer, *Codes as modules over skew polynomial rings*, Proceedings of the 12th IMA conference on Cryptography and Coding, Cirencester Lecture Notes in Computer Science, 5921, 38-55 (2009)

[5] L. Chaussade, *Codes correcteurs avec les polynômes tordus*, Thèse Université de Rennes 1, novembre 2010.

[6] L. Chaussade, P. Loidreau and F. Ulmer, *Skew codes of prescribed distance or rank*, Designs, Codes and Cryptography, 50(3), 267-284 (2009)

[7] P.M. Cohn, Free Rings and their relations, London Mathematical Society, 1971

[8] E.M. Gabidulin (1985), Theory of codes with maximum rank distance, *Probl. Peredach. Inform.,* **21**, 3–16 (in Russian; pp. 1–12 in the English translation).

[9] E.M. Gabidulin, A fast matrix decoding algorithm for rank-error-correcting codes. In : Cohen G., Litsyn S., Lobstein A., Zemor G. (eds) Lecture Notes in Computer Science, vol 573, pp. 126-133. Springer Verlag (1991)

[10] T.Y. Lam , *A general theory of Vandermonde matrices*, Expositiones Mathematicae 4, 193-215 (1986)

[11] T.Y. Lam and A. Leroy, *Vandermonde and Wronskian Matrices over Division Rings*, *Journal of Algebra,* **119** pp. 308-336 (1988)

[12] R. Lidl and H. Niederreiter, *Finite Fields.*, Encyclopedia of Mathematics and its Applications Vol. 20, Amsterdam: Addison-Wesley. (1956).

[13] P. Loidreau, A Welch-Berlekamp like algorithm for decoding Gabidulin codes *Lecture Notes in Comput. Sci., 2006*, 3969, 36–45

[14] O. Ore, Theory of Non-Commutative Polynomials, *The Annals of Mathematics*, 2nd Ser, Vol. 34, No. 3. pp 480-508 (1933)

[15] O. Ore, On a Special Class of Polynomials *Transactions of the American Mathematical Society*, Vol. 35, pp. 559-584, (1933).

[16] H. Wexler-Kreindler, *Sur une clasification des extension de Ore*, C.R. Ac. des Sciences Paris, Tome 282, pp. 133-1333 (1976)